修 士 論 文 の 和 文 要 旨

研究科・専攻	電気通信大学大学院 電気通信学研究科 情報工学専攻 博士前期課程		
氏 名	安達 悠	学籍番号	0731002
論 文 題 目	プロセスレベルの仮想化を用いたマルウェアの挙動解析システム		

要 旨

近年では，マルウェアの複雑化，多様化に伴い，攻撃者の意図を把握することが困難になってきている．攻撃者の意図を把握するためには，マルウェアの挙動を解析することが重要である．マルウェアや攻撃情報を収集・解析するための手法として，従来よりhoneypot が利用されてきた．

honeypot は，攻撃者に対するインタラクションレベルにおいて高対話型と低対話型に大別される．高対話型honeypot は，honeypot として本物のオペレーティングシステムやアプリケーションを利用するので，それらに対するマルウェアの挙動を観測することができる．しかし，多くのhoneypot を稼動させるためには多くの物理マシンが必要になる．一方，低対話型honeypot は，専用のスクリプト等によって，オペレーティングシステムやアプリケーションの動作をエミュレートする．これらは軽量だが，エミュレートした範囲でしか攻撃者をだますことができない．

本研究では，高対話型と低対話両方の欠点を補い，軽量かつ実アプリケーションに対するマルウェアの挙動を観測できるシステム *BitSaucer* をプロセスレベルの仮想化技術を用いて実現した．本システムは，1 台のマシン上に非常に多数の仮想環境を honeypot として動的に生成することができる．また，仮想的なファイルツリーを生成することと，マルウェアによる外部へのネットワーク接続を同一マシン内の仮想環境にリダイレクトすることにより，マルウェアを実環境から隔離する．本システムの利点は，少ない資源使用量とオーバーヘッドである．実際に，1 台のマシン上に 1,000 個の仮想環境を生成した場合でも，その環境内のアプリケーションは現実的な速度で正常に動作した．